REMARKS

In response to the Office Action mailed November 26, 2008, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks, have cancelled claims and have added new claims. The claims as now presented are believed to be in allowable condition.

Claims 1, 2, 4-28, 38 and 40-45 were pending in this Application. By this Amendment, claims 16 and 17 have been cancelled. Applicants expressly reserve the right to prosecute at least some of the canceled claims and similar claims in one or more related Applications. Claim 46 has been added. Accordingly, claims 1, 2, 4-15, 18-28, 38 and 40-46 are now pending in this Application. Claims 1, 9, 18, 19, 38, 40, 41, 43, and 45 are independent claims.

Rejections under §112

Claims 16-28 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to claim the subject matter that is the invention.

Claims 16 and 17 have been cancelled. Cancellation of claims 16 and 17 should in no way be construed as an acquiescence to the rejection but was done solely to expedite the prosecution of the application.

Claim 18 has been amended in accordance with the suggestions provided by the Office Action. The amendments to claim 18 do not add new matter to the Application. Accordingly, the rejection of claim 18 under 35 U.S.C. §112, second paragraph should be withdrawn.

Claim 19 has been amended in accordance with the suggestions provided by the Office Action. The amendments to claim 19 do not add new matter to the Application. Accordingly, the rejection of claim 19 under 35 U.S.C. §112, second

paragraph should be withdrawn. Because claims 20-28 depend from and further limit claim 19, claims 20-28 are in allowable condition for at least the same reasons.

Claim 24 was also amended to recite utilizing a Reed-Solomon error detecting code "to add redundancy symbols configured to correct errors in the first set of elements." Support for the amendment can be found in the Specification, for example, on page 12, lines 6-7. The amendment does not add new matter to the Application. Accordingly, the rejection of claim 24 under 35 U.S.C. §112, second paragraph should be withdrawn.

Rejections under §101

Claims 1, 2, 4-28, 38 and 40-45 were rejected under 35 U.S.C. §101 "because the claimed invention is directed to non-statutory subject matter." The Office Action asserts on page 5 that "the claims fail to recite a final result achieved by the invention that is useful, tangible, and concrete."

Independent claims 1, 9, 18, 19, 38, 40, 41, 43, and 45 have been amended to recite a final result that is "useful, tangible, and concrete." Taking claim 1 as an example, claim 1 has been amended to recite "utilizing the first sequence, in response to receiving a second input element from a user, to authenticate the user to a secured system associated with the first sequence." Support for the amendments is provided within the Specification, for example, on page 23, line 12-25. The Amendments do not add new matter to the Application. Accordingly, because claims 1, 9, 18, 19, 38, 40, 41, 43, and 45 recite a final result that is "useful, tangible, and concrete" (e.g., recite utilizing a particular output to authenticate a user) the rejection of claims 1, 9, 18, 19, 38, 40, 41, 43, and 45 under 35 U.S.C. §101 should be withdrawn. Because claims 2, 4-8, and 11-15 depend from and further limit claim 1, claims 2, 4-8, and 11-15 are in allowable condition for at least the same reasons. Because claims 20-28 depend

from and further limit claim 19, claims 20-28 are in allowable condition for at least the same reasons. Because claim 42 depends from and further limits claim 41, claim 42 is in allowable condition for at least the same reasons. Because claim 44 depends from and further limits claim 43, claim 44 is in allowable condition for at least the same reasons.

Rejections under §102

Claims 19-28 and 38 were rejected under 35 U.S.C. §102(b) as being anticipated by Juels et al., "A Fuzzy Commitment Scheme" (hereinafter Juels).

Applicants respectfully traverse each of these rejections and request reconsideration. The claims are in allowable condition.

Claim 19 relates to a computer-implemented method for generating an order invariant fuzzy commitment of an item of information, comprising receiving a first set of elements, selecting a polynomial for encoding the item under the first set of elements to generate an order-invariant fuzzy commitment of the item, generating the order-invariant fuzzy commitment of the item, storing said commitment in a computing device; and utilizing the commitment, in response to receiving a second set of elements from a user, to authenticate the user to a secured system associated with the commitment.

The Office Action has rejected claim 19 as being anticipated by Juels. However, claim 19 is patentable over Juels because Juels does not teach or suggest each element of Applicants' claim 19. For example, Juels does not teach or suggest "generating the order-invariant fuzzy commitment of the item" as claimed by Applicants.

Juels describes a fuzzy commitment scheme. In providing background to the fuzzy commitment scheme, Jules recites an overview of error correcting

codes on page 30, column 2, paragraphs 3-4. Here Juels recites the goal of an error correcting code is to enable transmission of a message m intact over a noisy channel. With error correcting codes, even if some bits of a string were corrupted by noise, it is possible for a receiver to reconstruct the message m.

While Juels recites the use of error correcting codes to allow communication over a noisy communication channel, Juels is in fact silent regarding the use of an *order-invariant* fuzzy commitment. Furthermore, the provisional application 60/253,291, to which the present Application claims priority, recites such a lack of teaching as one of the shortcomings of Juels. For example, page 3, paragraph 1 of the provisional application recites:

> The fuzzy commitment scheme of Juels and Wattenberg has two shortcomings. First, while it tolerates some number of errors in the information symbols in x, *it does not tolerate substantial re-ordering of these symbols*. Given that translation and rotation errors are common in biometric systems, it is not unreasonable to expect that the image x' may consist of a permutation of symbols in x. The property of order-invariance is thus likely to be desirable in a fuzzy commitment scheme. *Emphasis added.*

Because Juels does not teach or suggest the use of an order-invariant fuzzy commitment, Juels cannot teach or suggest "generating the order-invariant fuzzy commitment of the item" as claimed by Applicants.

For the reasons stated above, claim 19 patentably distinguishes over the cited prior art, and the rejection of claim 19 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claim 19 is in allowable condition. Because claims 20-28 depend from and further limit claim 19, claims 20-28 are in allowable condition for at least the same reasons.

Claim 38 relates to an article comprising a tangible machine readable medium that stores executable code instructions enabling a machine to perform

the steps of (a) receiving a first input element comprising a sequence of at least one value from a predetermined set, (b) generating a codeword of an error-correcting code, and (c) constructing a first sequence of coordinate sets, each of the coordinate sets having a first value corresponding to a representation of an associated one of the at least one value of the first input element and a second value corresponding to a symbol in the codeword, wherein the symbol is associated with the corresponding first value. The article further includes code for enabling the steps of receiving a second input element including a second sequence of at least one value from the predetermined set, receiving the order-invariant fuzzy commitment, constructing a set of values representing respectively the values in the second sequence, selecting a subset of the coordinate sets in the first sequence such that the first value in each subset coordinate set corresponds to the first value of at least one coordinate set in the first sequence, applying an error-correcting function to the subset, and authenticating a user associated with the second input element to a secured system associated with the first sequence.

The Office Action has rejected claim 38 as being anticipated by Juels. However, claim 38 is patentable over Juels because Juels does not teach or suggest each element of Applicants' claim 38. For example, Juels does not teach or suggest "receiving the order-invariant fuzzy commitment" as claimed by Applicants.

As indicated above, Juels does not teach or suggest the use of an order-invariant fuzzy commitment. Accordingly, Juels cannot teach or suggest "receiving the order-invariant fuzzy commitment" as claimed by Applicants.

For the reasons stated above, claim 38 patentably distinguishes over the cited prior art, and the rejection of claim 38 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claim 38 is in allowable condition.

Newly Added Claims

Claim 46 has been added and is believed to be in allowable condition. Claim 46 depends from claim 1. Support for claim 46 is provided within the Specification, for example, on page 7, lines 11-19 and page 23, lines 12-25. No new matter has been added.

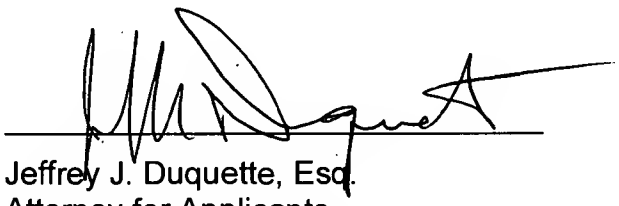
Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this effect is respectfully requested. If the Examiner believes, after this Response, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicants' Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Response, including an extension fee, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,



Jeffrey J. Duquette, Esq.
Attorney for Applicants
Registration No.: 45,487
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1048-016

Dated: February 26, 2009